CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION TECHNOLOGY

An Introduction to Acceptable Risk Safeguards (ARS) Version 3.0

Information Security & Privacy Group (ISPG)

Webinar
April 27, 2017
11:00 AM EDT

Meet Your Presenters

Clarence Mayfield

CMS ISPG
Privacy & Security
Policy Lead

Brett Kreider

ARS Tiger Team
SME, MITRE

Jason King

CMS ISPG
Cyber Risk Advisor
Team Lead

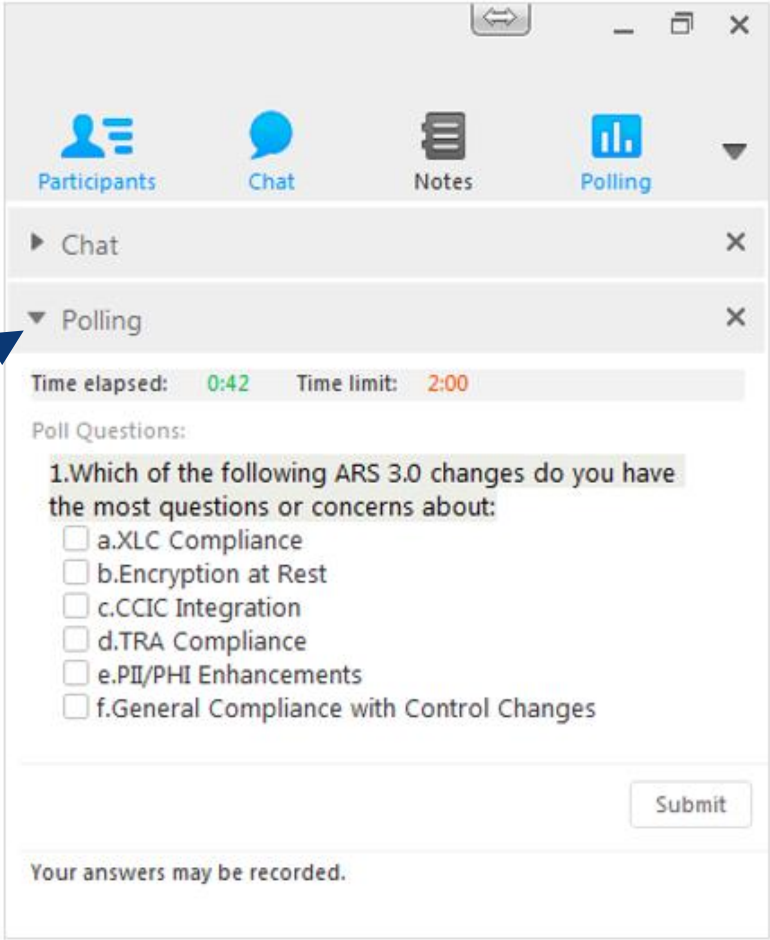
Today's Agenda

- About This Webinar
- Introduction to ARS 3.0
  - Policy Framework
  - Key Drivers
- Key Changes in ARS 3.0
  - Highlights and Enhancements
  - ARS 3.0 Change Overview
- Planning & Implementation to ARS 3.0
  - Rollout Timeline and Assessment
  - Use Cases
  - Resources
  - Q&A

About This Webinar

For Today's Webinar; How to Interact

Navigation Pane



Time elapsed: 0:42 Time limit: 2:00

Poll Questions:

1.Which of the following ARS 3.0 changes do you have the most questions or concerns about:

- □ a.XLC Compliance
- □ b.Encryption at Rest
- □ c.CCIC Integration
- □ d.TRA Compliance
- □ e.PII/PHI Enhancements
- □ f.General Compliance with Control Changes

Your answers may be recorded.

Click on the **Chat** menu to submit a question

Click on the **Polling** menu when prompted

Introduction to ARS 3.0; Objectives

This webinar will explore the drivers for, and changes to, the newly released CMS ARS 3.0 standard.

Upon completion, you will better understand the standard, ***and the options available for implementation***.

Today’s Webinar; Who is this for?

ISSOs

ISSOs are on the frontlines of ARS 3.0 implementation. This webinar will aid ISSOs in assessing and planning for necessary changes.

CMS Component Heads
Business Owners
System Owners
System Developers
& Maintainers

Many other stakeholders have key roles in implementing ARS 3.0. This webinar will provide information and tools to evaluate implementation planning.

Enhancing Cybersecurity is a Priority Across the Healthcare Sector (1)

CMS is in a Leadership Role

Medicare.gov

57.6 Million*

People Enrolled

*January 2017

Medicaid.gov
Keeping America Healthy

69 Million People Covered*

*December 2016 Enrollment Report

8.9 Million Children Enrolled*

* 2016 Statistical Enrollment Report

HealthCare.gov

9.2 Million*

People Signed-up for Coverage

*January 31, 2017

Enhancing Cybersecurity is a Priority Across the Healthcare Sector (2)

CMS is in a Leadership Role

144.7 Million People, or

45% of US Population

Entrusts CMS with their

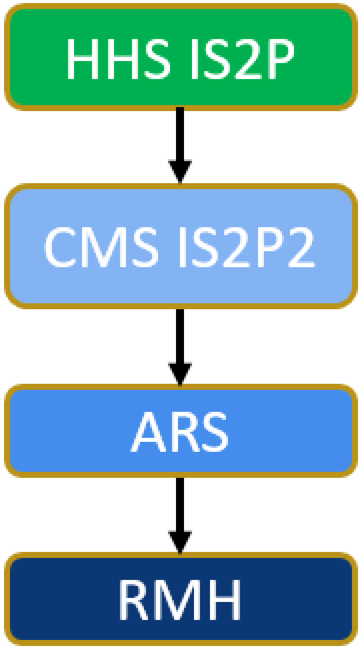
Protected Health Information (PHI) &

Personally Identifiable Information (PII)

Introduction to ARS 3.0

Policy Framework

- **Policy**
  - HHS Information System Security and Privacy Policy (IS2P)
  - CMS Information System Security and Privacy Policy (IS2P2)
    - Minimized duplication between documents
    - Provided authoritative references for any settings (IS2P2 or ARS 3.0) that are ***more stringent than the HHS IS2P***
- **Standards and Procedures**
  - Acceptable Risk Safeguards (ARS)
  - Risk Management Handbook (RMH)



Integrated Directives and Policies

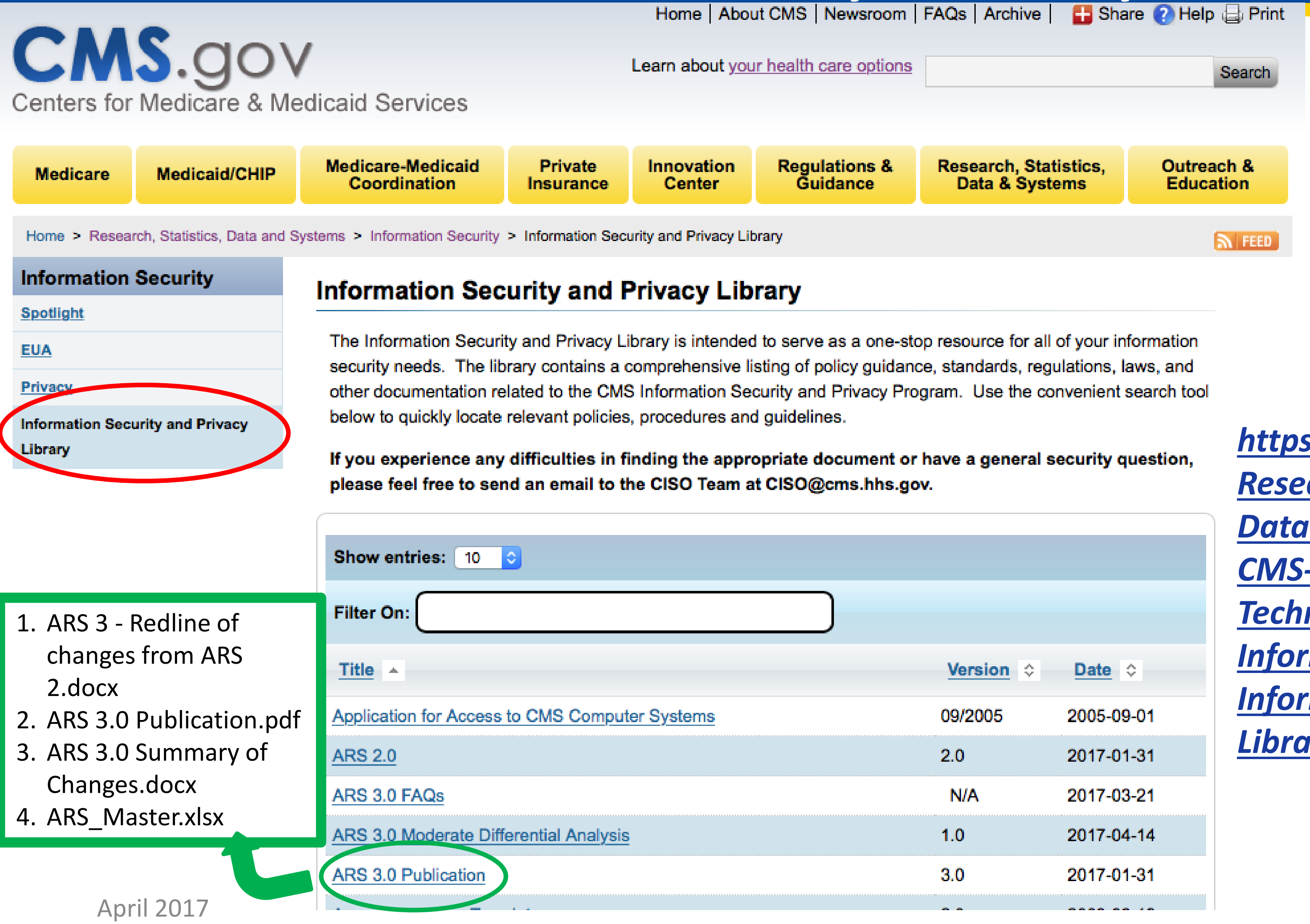
- CMS Policy for Information Security and Privacy, dated April 11, 2013
- CMS Policy for the Information Security Program, dated August 31, 2010
- CMS Master Security Plan, version 6.00, dated June 25, 2010
- CMS Policy for Privacy Act Implementation & Breach Notification, dated July 23, 2007
- CMS Policy for Cloud Computing 1.0, dated November 11, 2014 (CMS-CLD)
- CIO Directive 07-04, CMS Information Security Incident Handling and Breach Analysis/Notification Procedure, August 21, 2007 (Section 4.3)
- CIO Directive 12-01, CMS Vulnerability Assessment and Penetration Testing (ARS)
- CIO Directive 12-03, Annual Role-Based Information Security Training Requirements (4.1.5)
- CIO Directive 13-01, Policy for Monitoring Use of CMS IT Resources (4.1.1)
- CIO Directive 14-02, Cease Use of Windows XP, May 21, 2014 (ARS)
- CIO Directive 14-03, Interconnections, July 19, 2014 (4.1)
- CIO Directive 14-04, CMS Encryption of Sensitive Information in E-mail, November 13, 2014 (4.1)
- CIO Directive 15-01, Strong Authentication, June 26, 2015 (4.1)

Key Drivers for ARS 3.0

Simplifies compliance by consolidating requirements from multiple oversight documents

- HHS IS2P (published in 2014) and CMS IS2P2 (published 2016)
- Federal Cyber and Privacy Legislation & Guidance
  - OMB Circular A-130 expanding the role of the SAOP/SOP and enhanced privacy including **privacy continuous monitoring**
  - CNSS Privacy Guidance & Federal Privacy Council
  - OMB M-16-04, *Cybersecurity Strategy Implementation Plan (CSIP)* and M-17-09 emphasizing **High Value Asset** (HVA) Management
  - NIST Special Publication (SP) 800-53A (guidance for testing controls)
  - OMB M-14-03 and the Continuous Diagnostics and Mitigation (CDM) program emphasizing **Continuous Monitoring**
  - Newer guidance such as OMB M-17-06 for **Public Website Management** and M-17-12 on **Breach Response**
- CMS CIO Directives, Data Protection Initiative, and CCIC Integration Requirements (in the Technical Reference Architecture [TRA])

CMS Information Security and Privacy Library



Home | About CMS | Newsroom | FAQs | Archive | Share Help Print
CMS.gov
Centers for Medicare & Medicaid Services
Learn about your health care options
Search
Medicare
Medicaid/CHIP
Medicare-Medicaid Coordination
Private Insurance
Innovation Center
Regulations & Guidance
Research, Statistics, Data & Systems
Outreach & Education
Home > Research, Statistics, Data and Systems > Information Security > Information Security and Privacy Library
FEED
Information Security
Spotlight
EUA
Privacy
Information Security and Privacy Library

Information Security and Privacy Library

The Information Security and Privacy Library is intended to serve as a one-stop resource for all of your information security needs. The library contains a comprehensive listing of policy guidance, standards, regulations, laws, and other documentation related to the CMS Information Security and Privacy Program. Use the convenient search tool below to quickly locate relevant policies, procedures and guidelines.

If you experience any difficulties in finding the appropriate document or have a general security question, please feel free to send an email to the CISO Team at CISO@cms.hhs.gov.

Show entries: 10

Filter On:

Title	Version	Date
Application for Access to CMS Computer Systems	09/2005	2005-09-01
ARS 2.0	2.0	2017-01-31
ARS 3.0 FAQs	N/A	2017-03-21
ARS 3.0 Moderate Differential Analysis	1.0	2017-04-14
ARS 3.0 Publication	3.0	2017-01-31

1. ARS 3 - Redline of changes from ARS 2.docx
2. ARS 3.0 Publication.pdf
3. ARS 3.0 Summary of Changes.docx
4. ARS_Master.xlsx

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

ARS Structure

- Base Document (updated)
- Organized by NIST SP 800-53 Rev 4 Control Family
- Security Control Table

XX-##	**Control Title (High / Moderate / Low)**	**Priority**
Control Description (including PII, PHI, and CSP)		
Implementation Standards for H/M/L including PII (H/M), PHI (H/M), and CSP (H/M/L)		
Supplemental Guidance including PII, PHI, and CSP		
References		**Related Controls**
Assessment Objectives including PII, PHI, and CSP		
Assessment Methods and Objects including PII, PHI, and CSP		
Examine:	Interview:	Test:

Key Changes in ARS 3.0

ARS 3.0 Highlights (1)

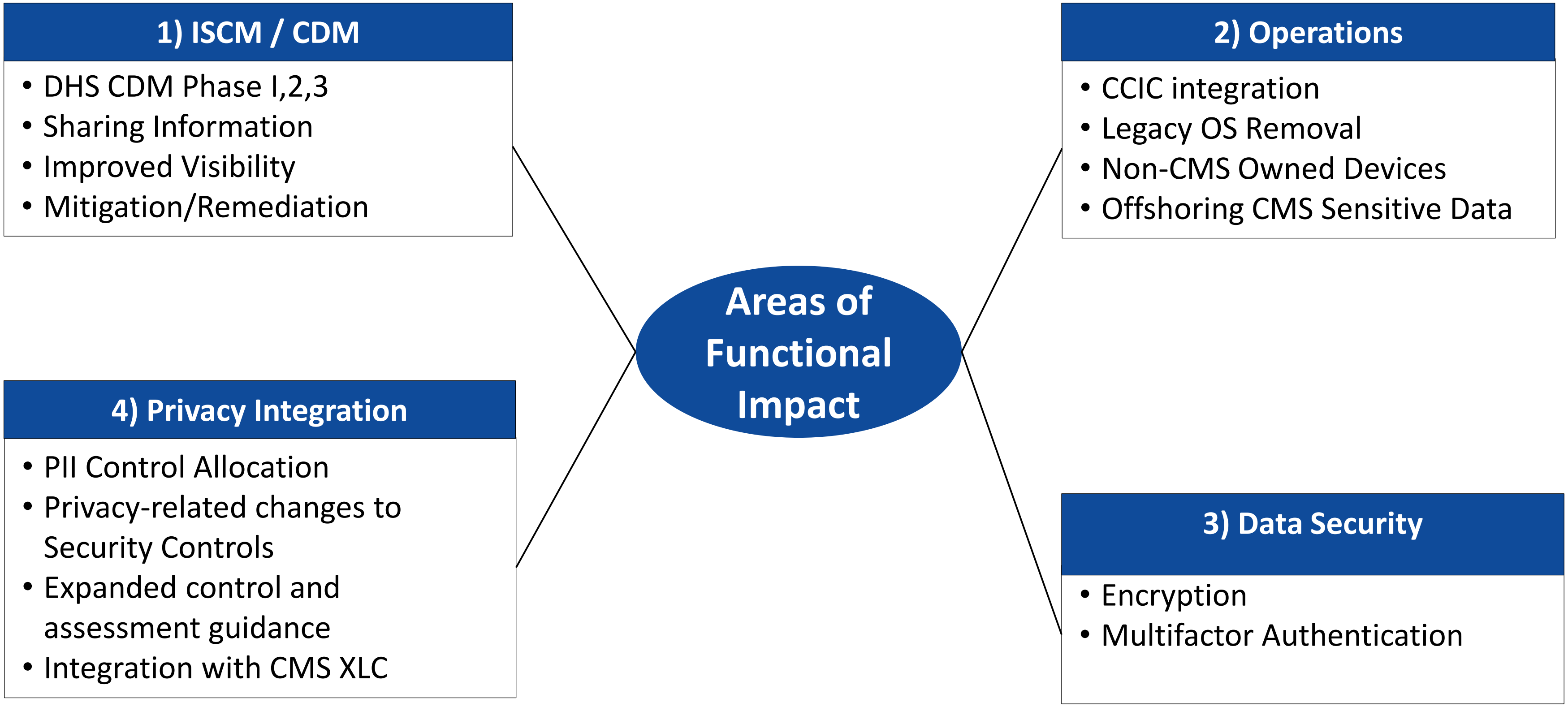
- Requires **encryption** of data at rest* and use of the latest **HHS Warning Banner**
- Provides guidance on how security controls **support privacy** including **privacy testing**
- Requires additional **security controls to protect Personally Identifiable Information (PII) and Protected Health Information (PHI)** (e.g., access control, audit, media protection)
- Centralizes data sharing to support **CMS Cybersecurity Integration Center** (CCIC) incident response, information sharing, and **Continuous Diagnostics and Mitigation** (CDM)
- Requires compliance with CMS's **Technical Reference Architecture (TRA)** and Expedited Lifecycle (**XLC**)

**HHS Standard for Encryption of Computing Devices and Information, December 14, 2016*

ARS 3.0 Highlights (2)

- Aligns **policy review period** with HHS requirement (every 3 years)
- Updates **Security Awareness Training** to cover email use, PII protection, and insider threat
- Clarifies the use of **connection agreements** (ISA, MOU, MOA, contractual clause, etc.)
- Clarifies **Security Assessment** guidance by enhancing **assessment methods and objects**

ARS 3.0 Highlights (3)



Areas of Functional Impact

1) ISCM / CDM

- DHS CDM Phase I,2,3
- Sharing Information
- Improved Visibility
- Mitigation/Remediation

2) Operations

- CCIC integration
- Legacy OS Removal
- Non-CMS Owned Devices
- Offshoring CMS Sensitive Data

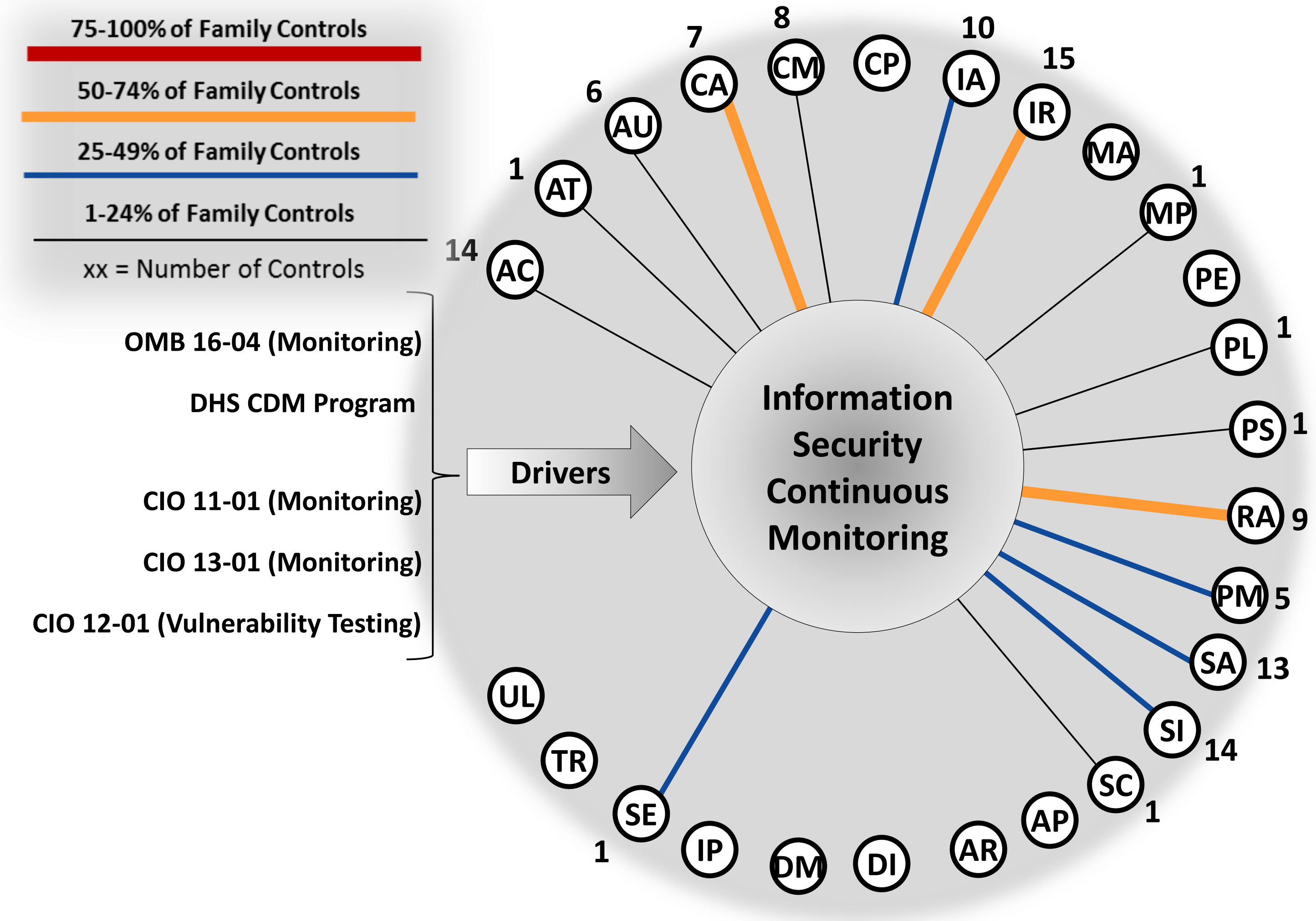
3) Data Security

- Encryption
- Multifactor Authentication

4) Privacy Integration

- PII Control Allocation
- Privacy-related changes to Security Controls
- Expanded control and assessment guidance
- Integration with CMS XLC

ARS 3.0 Impact on
1. ISCM-Related Controls



OMB 16-04 (Monitoring)

DHS CDM Program

CIO 11-01 (Monitoring)

CIO 13-01 (Monitoring)

CIO 12-01 (Vulnerability Testing)

DHS CDM Program evolution will drive additional ISCM-related control changes

IMPACT

- **Highest impact to CA, IR, and RA families**
- **No change to AP, AR CP, DI, DM, MA, PE, TR, and UL control families**

ARS 3.0 Impact on
2. Operations-Related Controls

75-100% of Family Controls 🟥

50-74% of Family Controls 🟧

25-49% of Family Controls 🟦

1-24% of Family Controls —

xx = Number of Controls

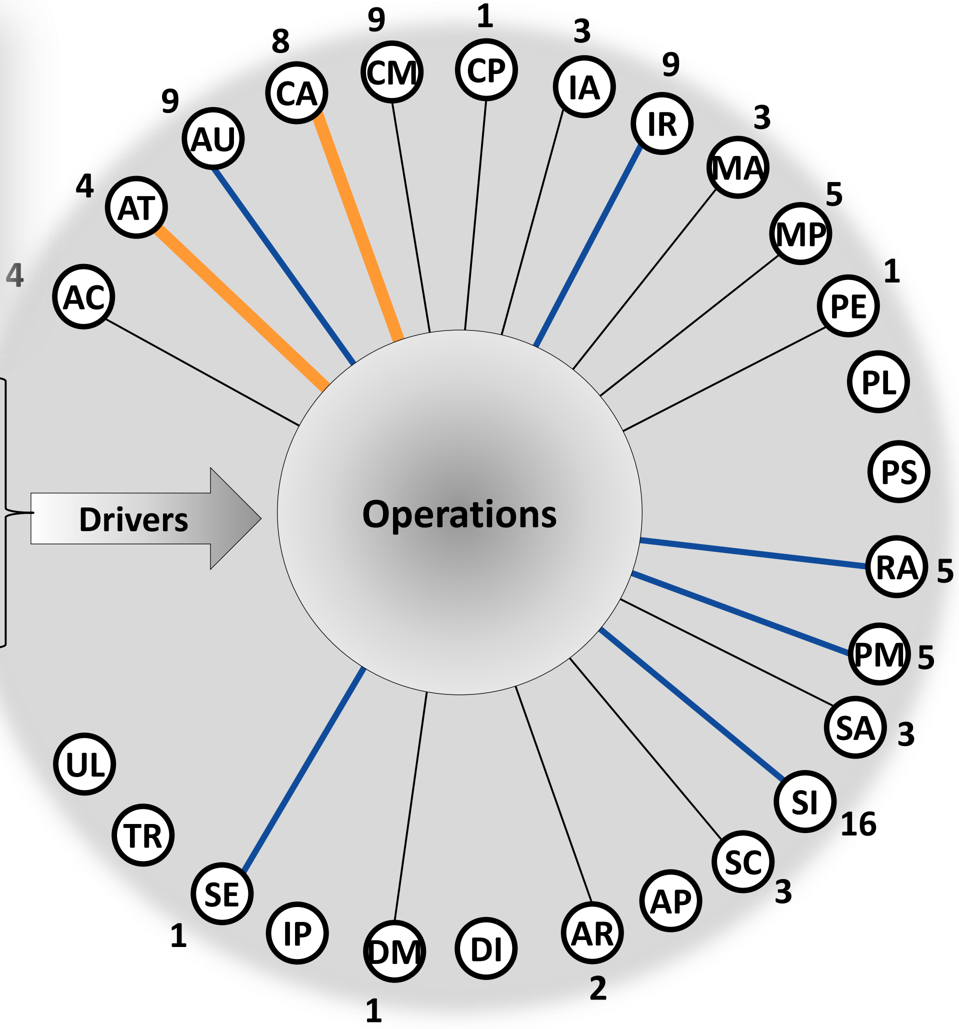
CCIC

RBT

CIO 07-04 (Incident Response)

CIO 14-03 (Interconnection)

SP 800-88 (Media Sanitization)

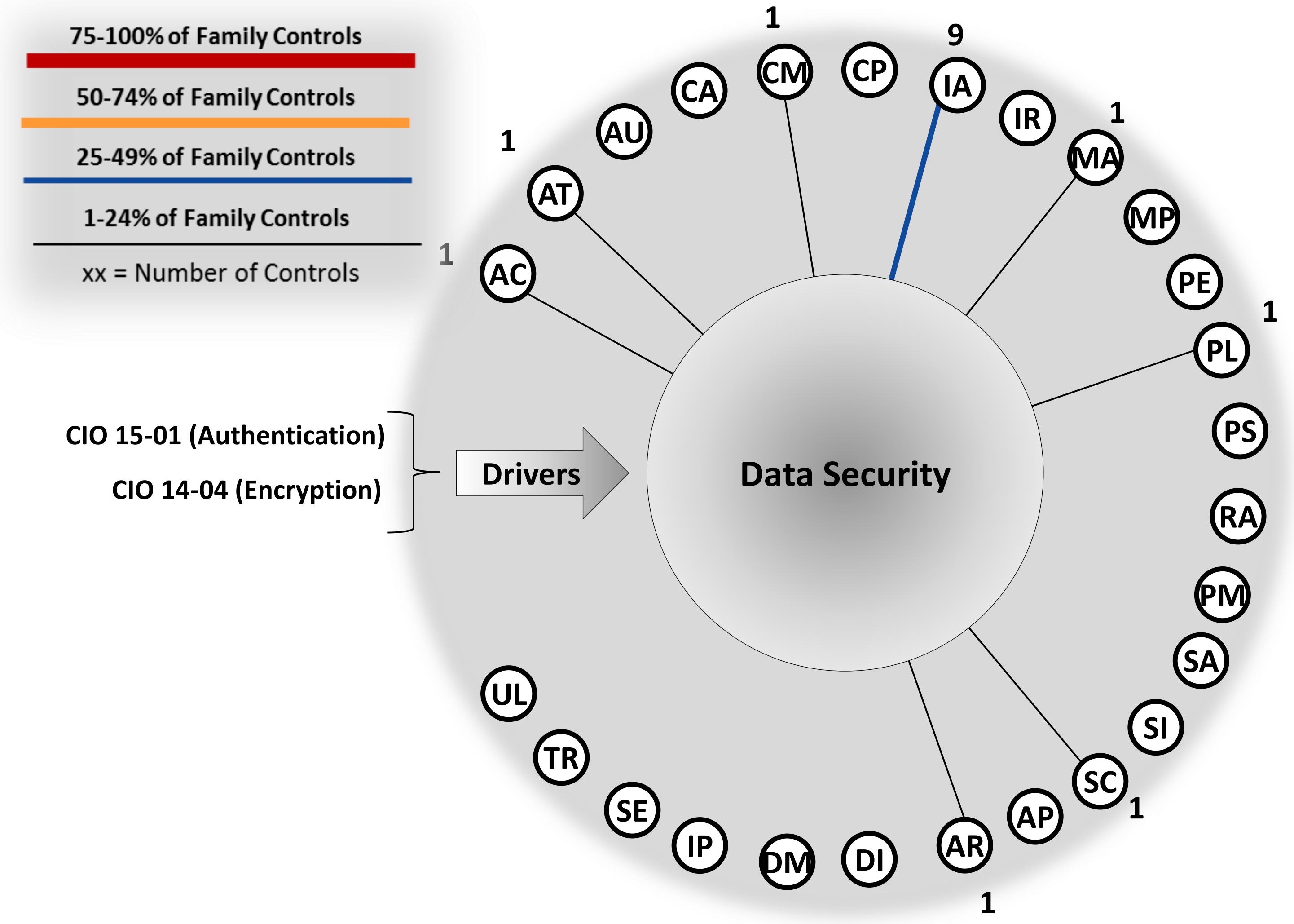


The CMS Cybersecurity Integration Center (CCIC) oversees ISPG's security operations capabilities

IMPACT

- **Highest impact to AT and CA controls**
- **No impact to AP, DI, IP, PL, PS, TR, and UL control families**

ARS 3.0 Impact on
3. Data Security



ARS Data Security includes both encryption and multifactor authentication (MFA) requirements

<u>IMPACT</u>

- **Highest impact to IA controls**
- **9 IA controls (> 25%) changed**
- **No privacy controls impacted**

ARS 3.0 Impact on
4. Privacy-Related Controls

🟥 75-100% of Family Controls

🟧 50-74% of Family Controls

🟦 25-49% of Family Controls

— 1-24% of Family Controls

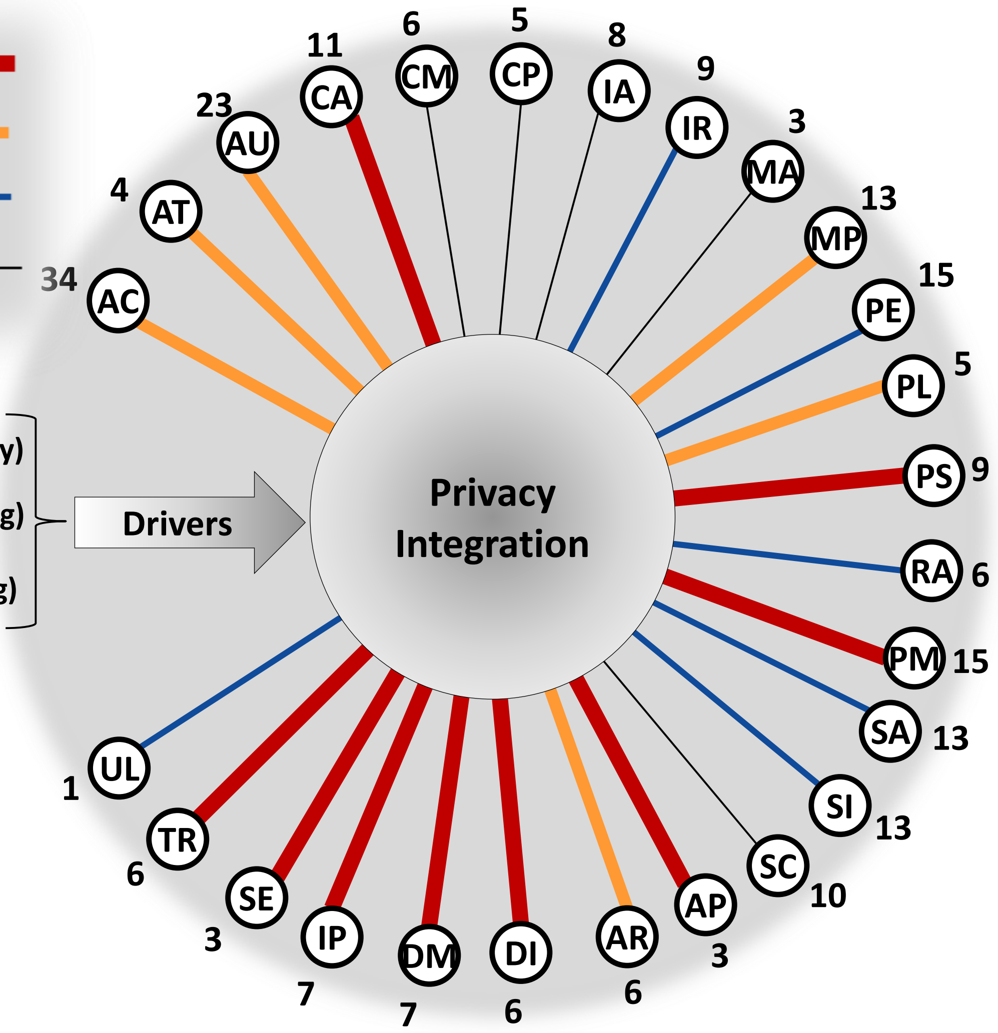
xx = Number of Controls

Privacy (CNSS Overlay)

CIO 12-03 (RBT Infosec Training)

CIO 12-01 (Vulnerability Testing)

Drivers



Privacy-related changes impact every control family

IMPACT

- Highest impact to CA, PS, PM, AP, DI, DM, IP, SE, TR, and UL families

- 34 (>50%) AC controls were updated or added

- 11 (>75%) of CA controls were updated

Differential Analysis

- **Audience**: ISSOs, CRAs, Privacy SMEs, Assessors
- **Purpose**: Tool to aid evaluation of system's implementation of the changes between ARS 2.0 and ARS 3.0 security controls.
    - **Modeled** after existing SCA evaluation template for SSP
    - **Highlights the differences** between ARS 2.0 and ARS 3.0
    - Clearly states **what actions (if any)** are required per control
    - Enables easy **identification** of non-compliance
    - Provides **narrative summary of changes** in each control
    - Guides Assessor to necessary **analysis steps**

Differential Analysis: Example

- **Red-highlighted text** indicates ARS 2 text that was **removed** or **replaced** in ARS 3
- **Green-highlighted text** indicates text added in ARS 3 that constitutes a **significant change** (one which **needs** to be assessed)
- **Pink-highlighted text** indicates text added in ARS 3 that constitutes an **insignificant change** (one which **does not need** to be assessed)
- **Yellow-highlighted bold text** indicates the key action/word for quick scanning

Control	Control Name	Category	ARS 2.0	ARS 3.0	Summary of Change	Assessment Guidance	Assessment Status	Assessment Comment
AC-2(2)	Removal of Temporary/ Emergency Accounts	Moderate	The information system automatically disables emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed **three hundred sixty-five (365) days**.	The information system automatically disables emergency accounts within 24 hours **for High and Moderate systems and 30 days for Low systems**; and temporary accounts with a fixed duration not to exceed **30 days for High systems and 60 days for Moderate or Low systems**.	*ARS 3* ***changes*** *the control by defining a shorter lifetime for emergency and temporary accounts.*	*Ensure records show temporary account and emergency account lifetimes do not exceed the limits specified.*	**Addressed**	**System XYZ disables emergency accounts at 12 hours, and temp accounts at 59 days.**
AC-2(2)	Removal of Temporary/ Emergency Accounts	CSP Moderate	Implementation Standards: **1. (For CSP only)** For service providers, the information system automatically disables temporary and emergency account types after no more than ninety (90) days.	Implementation Standards: **CSP.1** - For service providers, the information system automatically terminates temporary and emergency account types after no more than ninety (90) days.	***Insignificant*** *change.*	*No action required.*	**N/A**	**Not assessed.**

Differential Analysis: Availability

- **ISPG Created Individual Documents** for High, Moderate, and Low Systems
  - **High, Moderate, and Low**: available now from CMS Information Security and Privacy Library

Poll: Help Shape Future Webinars

Which of the following ARS 3.0 changes do you have the most questions or concerns about?

1. *Encryption at Rest*
2. *CCIC Integration*
3. *TRA Compliance*
4. *XLC Compliance*
5. *PII / PHI Enhancements*

Planning & Implementation

Transitioning Together

Path to Compliance:

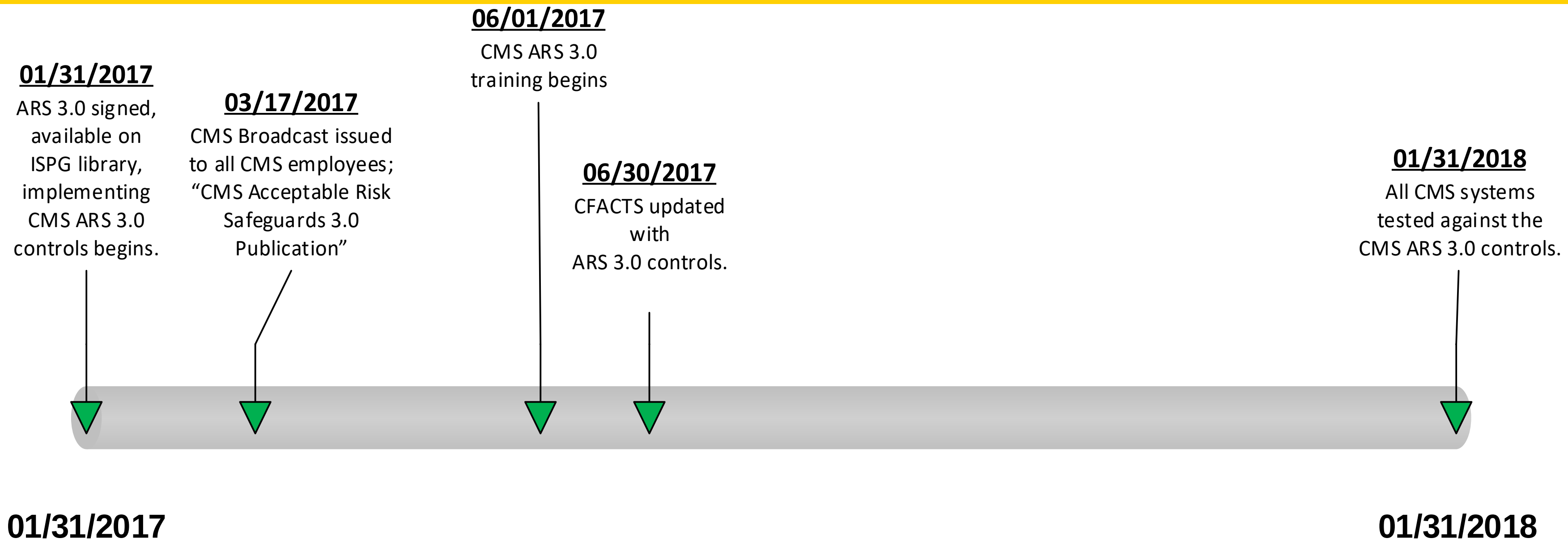
1. Know where you stand (by testing)
2. Have a plan (implementation options)

ISPG is here to help. Your Cyber Risk Advisor will:

- Evaluate your test results with you
- Evaluate implementation options with you to shape a plan that is both acceptable and least burdensome

CMS ARS 3.0 Rollout Schedule

(Source: CMS Broadcast dated March 17, 2017 from CMS Chief Information Officer



01/31/2017
ARS 3.0 signed, available on ISPG library, implementing CMS ARS 3.0 controls begins.

03/17/2017
CMS Broadcast issued to all CMS employees; "CMS Acceptable Risk Safeguards 3.0 Publication"

06/01/2017
CMS ARS 3.0 training begins

06/30/2017
CFACTS updated with ARS 3.0 controls.

01/31/2018
All CMS systems tested against the CMS ARS 3.0 controls.

01/31/2017

01/31/2018

Objective: Implement new Acceptable Risk Safeguards (3.0) to enhance cybersecurity to securely and confidentially treat sensitive and personal information that beneficiaries, recipients, providers and customers entrust to CMS.

Traceability to ISPG Cybersecurity & Privacy Strategy; Strategic Outcome 3, Full Operational Visibility of Sensitive Assets and Data, and Strategic Outcome 4, Risk-Based Governance and Engagement Practices

Assessment Stage

In what assessment stage is your system(s)?

A. *In development (No prior authorization)*

B. *1/3rd (One third)*

C. *2/3rd (Two third)*

D. *3/3 (Requires authorization)*

E. *Significant change*

F. *Assessment completed*

Use Cases

- System in Development
- Operation & Maintenance
  - 1/3
  - 2/3
  - 3/3 (Requires authorization)
  - Significant change
  - Assessment completed

System in Development

- Development System:
  - System in a pre-operational phase of XLC
  - Has not yet been issued an Authorization To Operate

Implementation Path:

- Implementation to ARS 3.0
- Assessment and Authorization to ARS 3.0

System in Operations & Maintenance: Testing to 1/3rd or 2/3rd

- System in O&M and testing in either the first or second year of the assessment cycle:
  - Has an existing ATO

Implementation Path (recommended):

- Test to ARS 3.0 differential
- Plan & Implement to ARS 3.0 differential
- Utilize the Plan of Action & Milestones process to prioritize ARS 3.0 implementation requirements

System in Operations & Maintenance: 3rd Year of Assessment

- System in O&M and in the third year of the assessment cycle:
  - Upcoming ATO Renewal

Implementation Path:

- Test ARS 3.0 differential
- Identify and test outlier controls that will not have be assessed over the three year cycle
- Utilize the Plan of Action & Milestones process to prioritize ARS 3.0 implementation requirements
- Prepare, submit Authorization package

System in Operations & Maintenance: Significant Change

- Operational system undergoing a significant change:
  - Will require an ATO

Implementation Path:

- Test ARS 3.0 differential
- Identify and test outlier controls impacted by the significant change
- Prepare and submit authorization package

All Stages: Assessment Completed

- Operational system that performed an annual assessment against ARS 2.0 prior to today.
- New system that performed a comprehensive assessment against ARS 2.0 prior to today.

Implementation Path:

- Work with your Cyber Risk Advisor and develop a plan to test ARS 3.0 controls.
- May include SCA or utilize services offered by ISPG such as penetration testing.

ARS 3 & CFACTS Highlights (1)

Schedule

- ARS 3 and CFACTS 2 in May
- ARS 3 and CFACTS 3 in July

What’s New

- Updated **CSP Questions** are on the **General Tab**
- New **PII Questions** added to **Security Category Tab** (answers pulled from PIA if it was filled out in PIA)
- New **PHI Questions** added to **Security Category Tab**
- Control Numbers on the Controls tab will look slightly different:
  - **From:** control number + security category (ie. AC-02 Mod) to
  - **To:** control number + security category + PII (if it has PII) + PHI (if it has PHI)

ARS 3 & CFACTS Highlights (2)

What's New

- The data required to be entered for each control will **remain the same** (i.e. inheritable, private implementation details, etc.)

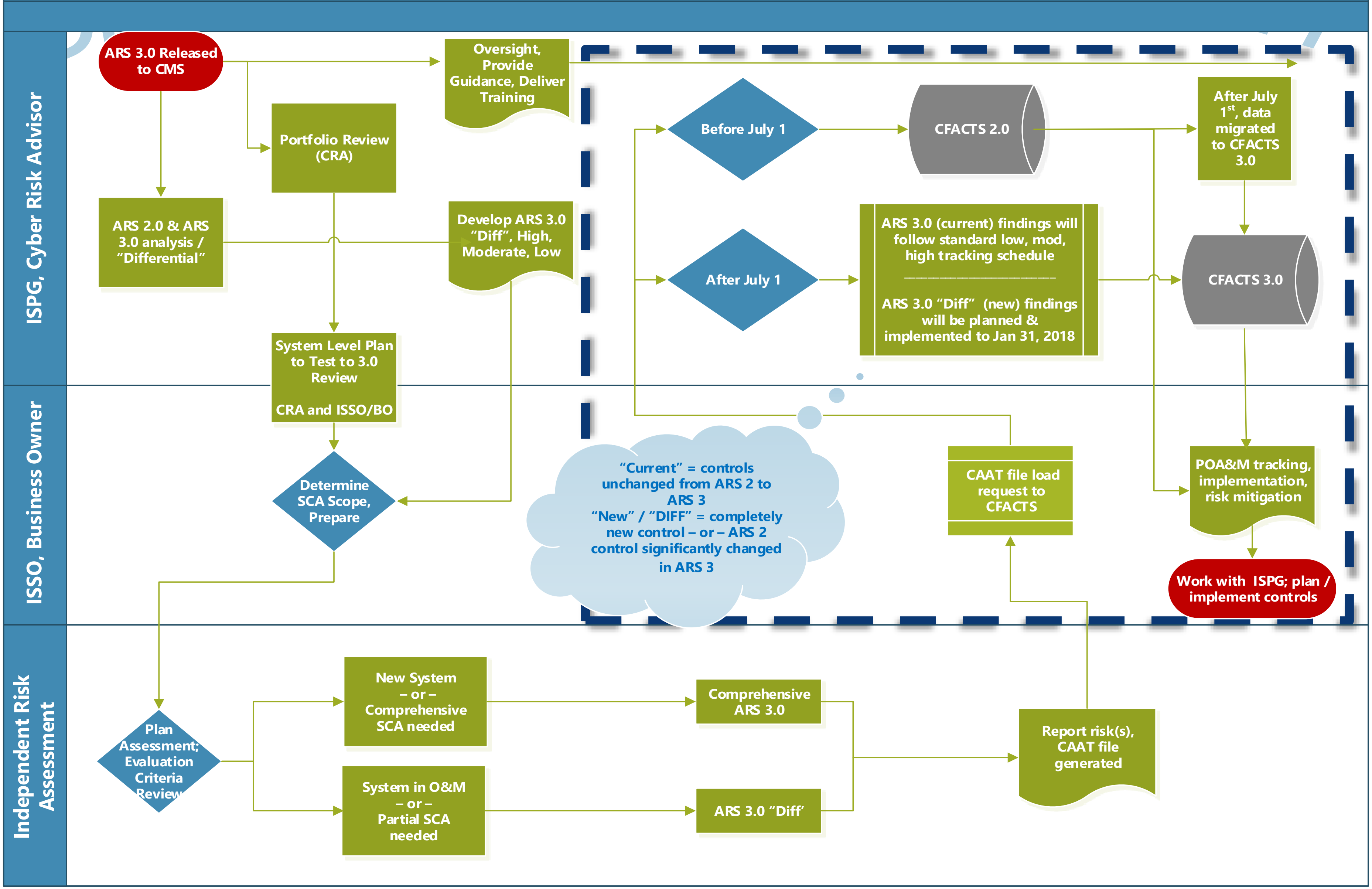
- All existing entered control data and CAAT/POA&M/Risk Acceptance records will be **transferred** to respective ARS 3 controls **by CFACTS team**

- CFACTS team data transfer from ARS 2 to ARS 3 will be executed one system at a time based upon system priority

  NOTE: This schedule is being developed, you will be notified once determined

- A **notification** will be sent **prior to and after** the data transfer.

ARS 3.0 Implementation, Standards, & Alignment to CFACTS 3.0 Release
April 18, 2017



ISPG, Cyber Risk Advisor

ARS 3.0 Released to CMS

ARS 2.0 & ARS 3.0 analysis / "Differential"

Portfolio Review (CRA)

Oversight, Provide Guidance, Deliver Training

Develop ARS 3.0 "Diff", High, Moderate, Low

System Level Plan to Test to 3.0 Review

CRA and ISSO/BO

Before July 1

CFACTS 2.0

After July 1st, data migrated to CFACTS 3.0

After July 1

ARS 3.0 (current) findings will follow standard low, mod, high tracking schedule

ARS 3.0 "Diff" (new) findings will be planned & implemented to Jan 31, 2018

CFACTS 3.0

ISSO, Business Owner

Determine SCA Scope, Prepare

"Current" = controls unchanged from ARS 2 to ARS 3

"New" / "DIFF" = completely new control – or – ARS 2 control significantly changed in ARS 3

CAAT file load request to CFACTS

POA&M tracking, implementation, risk mitigation

Work with ISPG; plan / implement controls

Independent Risk Assessment

Plan Assessment; Evaluation Criteria Review

New System – or – Comprehensive SCA needed

System in O&M – or – Partial SCA needed

Comprehensive ARS 3.0

ARS 3.0 "Diff'

Report risk(s), CAAT file generated

References, Resources

- CMS.gov, Information Security and Privacy Library https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

  Search for ARS 3.0 using the filter box
  - ARS 3.0 Publication
    - ARS 3.0 Summary of Changes
    - ARS 3 – Redline of changes from ARS 2
    - ARS Master
  - ARS-FAQs 3.0
  - ARS 3.0 Differential Analysis
- Your Cyber Risk Advisor

Privacy & Policy by Portfolio (1)
Your Dedicated Team

Component	Your Cyber Risk Advisor	Your Privacy Advisor
Center for Consumer Information and Insurance Oversight (CCIIO)	Kossi Azoumaro	Barbara Demopulos
Center of Clinical Standards and Quality (CCSQ)	Tony Oh	Chrislyn Gayhead
Consortium for Financial Management and Fee for Service Operations (CFMFFSO)	David Wheeler	Walter Stone
Center for Medicare (CM)	Joanna Pahl	Mike Pagels
Center for Medicare (CM)	Desmond Young	Mike Pagels
Center for Medicaid and CHIP Services (CMCS)	H. Michael Cohen	Barbara Demopulos
Center for Medicare & Medicaid Innovation (CMMI)	James Mensah	Amy Chapper
The Center for Program Integrity (CPI)	Robert Reintges	Walter Stone
The Center for Program Integrity (CPI)	Shawnte Garrett	Walter Stone
Federal Coordinated Health Care Office (FCHCO)	H. Michael Cohen	Mike Pagels
Office of the Actuary (OACT)	H. Michael Cohen	Amy Chapper
Office of Acquisition and Grants Management (OAGM)	H. Michael Cohen	Amy Chapper

Privacy & Policy by Portfolio (2)
Your Dedicated Team

Component	Your Cyber Risk Advisor	Your Privacy Advisor
Office of Communications (OC)	David Wheeler	Barbara Demopulos
Outpatient Code Editor (OCE)	Jason King	Mike Pagels
Office of Enterprise Data and Analytics (OEDA)	H. Michael Cohen	Walter Stone
Office of Financial Management (OFM)	James Mensah	Amy Chapper
Office of Human Capital (OHC)	Jason King	Amy Chapper
Offices of Hearings and Inquiries (OHI)	H. Michael Cohen	Amy Chapper
Office of Information Technology (OIT)	Joanna Pahl	Clarence Mayfield
Office of Information Technology (OIT)	Ken Daniels	Clarence Mayfield
Office of Information Technology (OIT)	Shawnte Garrett	Clarence Mayfield
Office of Legislation (OL)	Jason King	Amy Chapper
Office of Strategic Operations and Regulatory Affairs (OSORA)	H. Michael Cohen	Chrislyn Gayhead
Office of Support Services and Operations (OSSO)	Jason King	Chrislyn Gayhead

Questions

Stay Tuned

This presentation will be posted on the CMS Information Security and Privacy Library, along with the Q&A from this event.

Additional training will be coming soon to address specific areas of focus during ARS 3.0 planning and implementation

Thank You

CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION TECHNOLOGY